REMARKS

The Examiner has rejected Claims 41 and 68 under 35 U.S.C. 112, first paragraph, as being not enabled. Applicant respectfully asserts that such rejection is moot in view of the cancellation of such claims.

The Examiner has rejected Claims 1, 3, 5-10, 12, 14-18, 20, 22-26, 28-33, 35-39, 41-46, 48-51 and 53-70 under 35 U.S.C. 103(a) as being unpatentable over Brothers (U.S. Patent No. 5,799,083) in view of Barton (U.S. Patent No. 5,912,972). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to incorporate the subject matter of dependent Claim 8 et al.

With respect to independent Claim 1 et al., the Examiner has relied, at least in part, on the following excerpts from Barton and Brothers to meet applicant's claimed "verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame, and comparing the verification cryptographic hash and the original cryptographic hash" (see this or similar, but not identical, language in each of the independent claims).

> "A suitable **algorithm for calculating a digital signature** generates a representation that is not reproducible except from the original data. Examples of digital signatures include a checksum, which is good for small blocks of data; a cyclic redundancy check (CRC), which provides a much better signature over larger blocks of data..." (Barton-Col. 4, lines 1-7-emphasis added)
>
> "The invention provides a method and apparatus for basic authentication of a digital block and for carrying additional authentication information provided by the user, i.e. meta-data, in a secure and reliable fashion. **To embed authentication data into a digital block, a digital signature is formed** that is a reduced representation of the digital block. The signature and

> additional information supplied by the user are embedded into the digital block by replacing predetermined bits within the block. Encryption can be used to enhance authentication capability." (Barton-Col. 4, lines 18-27)
>
> "...a sequence numbers can also be provided as part of the meta-data..." (Barton-Col. 4, line 30-emphasis added)
>
> "Uniqueness: The block size must be chosen to match the digital signature technique, or vice-versa. The goal is to **achieve as unique a signature as possible**, within the bounds of cost and efficiency. For instance, a 16-bit checksum is appropriate for very small blocks (e.g. a few tens of bytes) and is also very quickly calculated, while a Fourier transform is appropriate for very large blocks, but takes a great amount of time to calculate." (Barton-Col. 6, lines 37-44-emphasis added)
>
> "is simply played back on a video player that **decodes the tape using the public key** that is supplied by the trusted third party 12 and referenced by the key's identification code. It is essential that the party performing the verification ascertains that the public key itself is authentic." (Brothers-Col. 8, lines 23-27-emphasis added)

Applicant respectfully asserts that the above excerpts simply teach digital signatures that are used to authenticate data and then decoding a tape with a public key (see emphasized excerpts above). Such teaching simply does not meet the level of specificity of applicant's claim language. Particularly, Barton's and Brothers' general teaching of a digital signature used to authenticate data and a public key used to decode a tape simply does not meet applicant's claimed "verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame, and comparing the verification cryptographic hash and the original cryptographic hash" (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined)

must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claim 8 et al. into each of the independent claims.

With respect to dependent Claim 8 et al., presently incorporated into each of the independent claims, the Examiner has relied on the following excerpt from Brothers to make a prior art showing of applicant's claimed "a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key" (see this or similar, but not identical, language in each of the foregoing claims).

> "...at least one programmable memory to store at least one cryptographic key for use with the encryption and decryption algorithms." (Col. 1, lines 59-61)

Applicant respectfully asserts that the above excerpt from Brothers does not meet applicant's specific claim language. In particular, Brothers' programmable memory clearly does not rise to the level of specificity of applicant's "removable storage medium" (emphasis added). Allowing a cryptographic key to be stored on a programmable memory simply does not inherently allow for storing at least one of an encryption cryptographic key and a decryption cryptographic key on a removable storage medium such that they can be removed from the system, as provided for in applicant's claim language.

A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to dependent Claim 9 et al., the Examiner has relied on the following excerpt from Barton to make a prior art showing of applicant's claimed "set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key" (see this or similar, but not identical, language in each of the foregoing claims).

"...append to the string to be embedded a bit string indicating the encryption technique employed." (Col. 7, lines 24-25)

Applicant respectfully asserts that the above excerpt from Barton not only fails to teach applicant's claim language, but *teaches away* from applicant's specific claim language. Barton teaches embedding a string indicating the encryption technique employed, where "the embedding process modifies the data block in place to contain the embedded information" (see Col. 6, lines 63-65). Applicant respectfully asserts that embedding the string into the data block teaches away from applicant's claim language since a string could not simultaneously be embedded in the data, as in Barton, and also stored on a removable storage medium, as claimed by applicant. In addition, applicant claims that "a set of cryptographic instructions are stored on the removable storage medium" (emphasis added), and not simply the encryption technique employed, as taught in Barton.

Since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a specific prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P383/01.023.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100